

## **AMENDMENTS TO THE CLAIMS**

**1. (Currently Amended)** A key agreement system comprising a shared-key generation apparatus and a shared-key recovery apparatus, each apparatus establishing therein a same shared key in secrecy,

wherein the shared-key generation apparatus includes:

a seed-value generating unit ~~operable~~ configured to generate a seed value;

a first shared-key generating unit ~~operable~~ configured to generate a verification value and a shared key, from the seed value;

a first encryption unit ~~operable~~ configured to encrypt the verification value to generate first encryption information;

a second encryption unit ~~operable~~ configured to encrypt the seed value based on the verification value, to generate second encryption information; and

a transmitting unit ~~operable~~ configured to transmit to the shared-key recovery apparatus the first encryption information and the second encryption information without transmitting to the shared-key recovery apparatus the generated shared-key,

wherein the shared-key recovery apparatus includes:

a receiving unit ~~operable~~ configured to receive from the shared-key generation apparatus the first encryption information and the second encryption information;

a first decryption unit ~~operable~~ configured to decrypt the first encryption information, to generate a first decryption verification value;

a second decryption unit ~~operable~~ configured to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value;

a second shared-key generating unit ~~operable~~ configured to generate a second decryption verification value and a decryption shared key, from the decryption seed value

~~and~~ according to ~~[[a]]~~ the same method as used in the first shared-key generating unit of the shared-key generation apparatus; and

a judging unit ~~operable~~ configured to judge whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification value, and to judge that the decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted; and

~~an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key;~~

~~wherein the shared-key generation apparatus and the shared-key recovery apparatus are separate apparatuses~~ the shared-key generation apparatus is distinct from the shared-key recovery apparatus, and

~~wherein the first encryption information and the second encryption information are separate pieces of information~~ the first encryption information is distinct from the second encryption information.

**2. (Currently Amended)** The key agreement system of claim 1,

wherein the shared-key generation apparatus further includes:

an obtaining unit ~~operable~~ configured to obtain a content; and

an encryption unit ~~operable~~ configured to encrypt the obtained content using the

shared key, to generate an encrypted content,

wherein the transmitting unit further transmits to the shared-key recovery apparatus the encrypted content, and

~~the receiving unit further receives the encrypted content, and~~

wherein the shared-key recovery apparatus further includes:

a decryption unit, ~~operable~~ when the receiving unit receives from the shared-key generation apparatus the encrypted content, configured to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content; ~~and~~  
~~an outputting unit operable to output the decrypted content.~~

**3. (Currently Amended)** A shared-key generation apparatus ~~that notifies the shared-key recovery apparatus about a shared key in secrecy, the shared-key generation apparatus~~ comprising:

a seed-value generating unit ~~operable~~ configured to generate a seed value;

a shared-key generating unit ~~operable~~ configured to generate a verification value and a shared key, from the seed value;

a first encryption unit ~~operable~~ configured to encrypt the verification value to generate first encryption information;

a second encryption unit ~~operable~~ configured to encrypt the seed value based on the verification value, to generate second encryption information; and

a transmitting unit ~~operable~~ configured to transmit to a shared-key recovery apparatus the first encryption information and the second encryption information without transmitting to the shared-key recovery apparatus the generated shared-key,

wherein the shared-key recovery apparatus decrypts the first encryption information to generate a first decryption verification value, decrypts the second

encryption information based on the first decryption verification value to generate a decryption seed value, generates a second decryption verification value and a decryption shared key from the decryption seed value according to the same method as used in the shared-key generating unit of the shared-key generation apparatus, judges whether the first decryption verification value is identical to the second decryption verification value, and judges that the generated decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value,

~~wherein the shared-key generation apparatus and the shared-key recovery apparatus are separated apparatuses~~ the shared-key generation apparatus is distinct from the shared-key recovery apparatus, and

~~wherein the first encryption information and the second encryption information are separate pieces of information~~ the first encryption information is distinct from the second encryption information.

**4. (Original)** The shared-key generation apparatus of claim 3, wherein the seed-value generating unit generates a random number, as the seed value.

**5. (Original)** The shared-key generation apparatus of claim 3, wherein the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value and the shared key from the functional value.

**6. (Original)** The shared-key generation apparatus of claim 5, wherein the shared-key generating unit performs, on the seed value, a hash function as the one-way

function, to generate the functional value.

**7. (Original)** The shared-key generation apparatus of claim 5, wherein the shared-key generating unit generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key.

**8. (Original)** The shared-key generation apparatus of claim 3, wherein the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the verification value, the shared key, and a blind value, from the functional value.

**9. (Currently Amended)** The shared-key generation apparatus of claim 8, wherein the first encryption unit includes:

- a public-key obtaining subunit ~~operable~~ configured to obtain a public key; and
- a public-key encryption subunit ~~operable~~ configured to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information.

**10. (Original)** The shared-key generation apparatus of claim 9, wherein

- the public-key encryption algorithm conforms to an NTRU cryptosystem,
- the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, and
- the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and

encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial.

**11. (Currently Amended)** The shared-key generation apparatus of claim 3, wherein the first encryption unit includes:

a public-key obtaining subunit ~~operable~~ configured to obtain a public key; and  
a public-key encryption subunit ~~operable~~ configured to perform a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information.

**12. (Original)** The shared-key generation apparatus of claim 11, wherein  
the public-key encryption algorithm conforms to an NTRU cryptosystem,  
the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, and  
the public-key encryption subunit generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial.

**13. (Original)** The shared-key generation apparatus of claim 3, wherein  
the second encryption unit performs a one-way function on the verification value

to generate a functional value, and performs an encryption algorithm, on the seed value, using the functional value, to generate the second encryption information.

**14. (Original)** The shared-key generation apparatus of claim 13, wherein the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information.

**15. (Original)** The shared-key generation apparatus of claim 13, wherein the second encryption unit performs a symmetric key encryption algorithm as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information.

**16. (Original)** The shared-key generation apparatus of claim 13, wherein the second encryption unit performs addition as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information.

**17. (Original)** The shared-key generation apparatus of claim 13, wherein the second encryption unit performs multiplication as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information.

**18. (Original)** The shared-key generation apparatus of claim 13, wherein the second encryption unit performs, on the verification value, a hash function as the one-way function, to generate the functional value.

**19. (Original)** The shared-key generation apparatus of claim 3, wherein the second encryption unit performs an encryption algorithm on the seed value using the verification value, to generate the second encryption information.

**20. (Original)** The shared-key generation apparatus of claim 3, wherein the second encryption unit encrypts the seed value using the verification value and the first encryption information.

**21. (Original)** The shared-key generation apparatus of claim 20, wherein the second encryption unit performs a one-way function on the verification value and the first encryption information, to generate the functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information.

**22. (Original)** The shared-key generation apparatus of claim 21, wherein the second encryption unit performs bitwise exclusive-or as the encryption algorithm, on the functional value and the seed value, to generate the second encryption information.

**23. (Currently Amended)** The shared-key generation apparatus of claim 3, further comprising:

- an obtaining unit ~~operable~~ configured to obtain a content; and
- an encryption unit ~~operable~~ configured to encrypt the obtained content using the shared key, to generate an encrypted content, wherein

the transmitting unit further transmits the encrypted content to the shared-key



recovery apparatus.

**24. (Currently Amended)** A shared-key recovery apparatus that receives information regarding a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting to the shared-key recovery apparatus the first encryption information and the second encryption information without transmitting to the shared-key recovery apparatus the generated shared-key, the shared-key recovery apparatus comprising:

a receiving unit ~~operable~~ configured to receive from the shared-key generation apparatus the first encryption information and the second encryption information;

a first decryption unit ~~operable~~ configured to decrypt the first encryption information, to generate a first decryption verification value;

a second decryption unit ~~operable~~ configured to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value;

a shared-key generating unit ~~operable~~ configured to generate a second decryption verification value and a decryption shared key, from the decryption seed value ~~and~~ according to [[a]] the same method as used in the shared-key generation apparatus;

a judging unit ~~operable~~ configured to judge whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption

information and the first decryption verification value, and to judge that the decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted; and

~~an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key;~~

~~wherein the shared-key generation apparatus and the shared-key recovery apparatus are separated apparatuses~~ the shared-key generation apparatus is distinct from the shared-key recovery apparatus, and

~~wherein the first encryption information and the second encryption information are separate pieces of information~~ the first encryption information is distinct from the second encryption information.

**25. (Currently Amended)** The shared-key recovery apparatus of claim 24, wherein

the shared-key generation apparatus obtains a public key, and performs a public-key encryption algorithm on the verification value, using the public key, to generate the first encryption information, and

the first decryption unit includes:

a secret-key obtaining subunit ~~operable~~ configured to obtain a secret key that corresponds to the public key; and

a public-key decryption subunit ~~operable~~ configured to perform a public-key decryption algorithm on the first encryption information, to generate

the first decryption verification value, the public-key decryption algorithm corresponding to the public-key encryption algorithm.

**26. (Previously Presented)** The shared-key recovery apparatus of claim 25, wherein

the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem,

the shared-key generation apparatus obtains, as the public key, a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial,

the receiving unit receives the first encryption information as a polynomial,

the secret-key obtaining subunit obtains, as the secret key, a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, and

the public-key decryption subunit decrypts the first encryption information as a polynomial, according to a decryption algorithm corresponding to the NTRU cryptosystem's encryption algorithm, using the secret-key polynomial as a key, to generate a decryption verification-value polynomial, and generates the first decryption verification value from the decryption verification-value polynomial.

**27. (Original)** The shared-key recovery apparatus of claim 24, wherein  
the shared-key generation apparatus performs a one-way function on the  
verification value, to generate a functional value, and performs an encryption algorithm on  
the seed value using the functional value, to generate the second encryption information,  
and

the second decryption unit performs the one-way function on the first decryption  
verification value, to generate a decryption functional value, and performs, on the second  
encryption information, a decryption algorithm corresponding to the encryption algorithm,  
using the decryption functional value, to generate the decryption seed value.

**28. (Original)** The shared-key recovery apparatus of claim 27, wherein  
the shared-key generation apparatus performs, on the functional value and the  
seed value, bitwise exclusive-or as the encryption algorithm, to generate the second  
encryption information, and

the second decryption unit performs, on the decryption functional value and the  
second encryption information, bitwise exclusive-or as the decryption algorithm, to  
generate the decryption seed value.

**29. (Original)** The shared-key recovery apparatus of claim 27, wherein  
the shared-key generation apparatus performs, on the functional value and the  
seed value, a symmetric key encryption algorithm as the encryption algorithm, to generate  
the second encryption information, and

the second decryption unit performs, on the decryption functional value and the  
second encryption information, a symmetric key decryption algorithm as the decryption  
algorithm, to generate the decryption seed value, the symmetric key decryption algorithm

corresponding to the symmetric key encryption algorithm.

**30. (Original)** The shared-key recovery apparatus of claim 27, wherein the shared-key generation apparatus performs, on the functional value and the seed value, addition as the encryption algorithm, to generate the second encryption information, and the second decryption unit performs, on the decryption functional value and the second encryption information, subtraction as the decryption algorithm, to generate the decryption seed value.

**31. (Original)** The shared-key recovery apparatus of claim 27, wherein the shared-key generation apparatus performs, on the functional value and the seed value, multiplication as the encryption algorithm, to generate the second encryption information, and the second decryption unit performs, on the decryption functional value and the second encryption information, division as the decryption algorithm, to generate the decryption seed value.

**32. (Original)** The shared-key recovery apparatus of claim 27, wherein the shared-key generation apparatus performs, on the verification value, a hash function as the one-way function, to generate the functional value, and the second decryption unit performs, on the first decryption verification value, the hash function as the one-way function, to generate the decryption functional value.

**33. (Original)** The shared-key recovery apparatus of claim 24, wherein the shared-key generation apparatus performs an encryption algorithm on the seed

value using the verification value, to generate the second encryption information, and  
the second decryption unit performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information using the first decryption verification value, to generate the decryption seed value.

**34. (Original)** The shared-key recovery apparatus of claim 24, wherein  
the shared-key generation apparatus encrypts the seed value using the verification value and the first encryption information, and  
the second decryption unit decrypts the second encryption information, using the first decryption verification value and the first encryption information, to generate the decryption seed value.

**35. (Original)** The shared-key recovery apparatus of claim 34, wherein  
the shared-key generation apparatus performs a one-way function on the verification value and the first encryption information, to generate a functional value, and performs an encryption algorithm on the seed value using the functional value, to generate the second encryption information, and  
the second decryption unit performs the one-way function on the first decryption verification value and the first encryption information, to generate a decryption functional value, and performs a decryption algorithm corresponding to the encryption algorithm, on the second encryption information, using the decryption functional value, to generate the decryption seed value.

**36. (Original)** The shared-key recovery apparatus of claim 35, wherein the shared-key generation apparatus performs bitwise exclusive-or as the encryption algorithm,

on the functional value and the seed value, to generate the second encryption information, and

the second decryption unit performs bitwise exclusive-or as the decryption algorithm, on the decryption functional value and the second encryption information, to generate the decryption seed value.

**37. (Original)** The shared-key recovery apparatus of claim 24, wherein

the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, and generates the verification value and the shared key from the functional value, and

the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates the second decryption verification value and the decryption shared key from the decryption functional value.

**38. (Original)** The shared-key recovery apparatus of claim 37, wherein

the shared-key generation apparatus performs, on the seed value, a hash function as the one-way function, to generate the functional value, and

the shared-key generating unit performs, on the decryption seed value, the hash function as the one-way function, to generate the decryption functional value.

**39. (Original)** The shared-key recovery apparatus of claim 37, wherein

the shared-key generation apparatus generates the verification value by setting a part of the functional value as the verification value, and generates the shared key by setting another part of the functional value as the shared key, and

the shared-key generating unit generates the second decryption verification value

by setting a part of the decryption functional value as the second decryption verification value, and generates the decryption shared key by setting another part of the decryption functional value as the decryption shared key.

**40. (Original)** The shared-key recovery apparatus of claim 24, wherein  
the shared-key generation apparatus performs a one-way function on the seed value, to generate a functional value, generates the verification value, the shared key, and a blind value, from the functional value, obtains a public key, and performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information, and  
the shared-key generating unit performs the one-way function on the decryption seed value, to generate a decryption functional value, and generates, from the decryption functional value, the second decryption verification value, the decryption shared key, and the decryption blind value.

**41. (Currently Amended)** The shared-key recovery apparatus of claim 40, wherein  
the shared-key generation apparatus obtains a public key, performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information, and  
the judging unit, instead of performing the judging based on the first decryption verification value and the second decryption verification value, includes:  
a public-key obtaining subunit ~~operable~~ configured to obtain the public key;  
a re-encryption subunit ~~operable~~ configured to perform the public-key encryption algorithm on one of the first decryption verification value and the second decryption



verification value, using the public key and the decryption blind value, to generate re-encryption information; and

a judging subunit ~~operable~~ configured to judge, based on the first encryption information and the re-encryption information, whether the decryption shared key should be outputted or not.

**42. (Original)** The shared-key recovery apparatus of claim 41, wherein the judging subunit compares the first encryption information and the re-encryption information, thereby judging that the decryption shared key should be outputted if the first encryption information is identical to the re-encryption information.

**43. (Original)** The shared-key recovery apparatus of claim 41, wherein the public-key encryption algorithm conforms to an NTRU cryptosystem, the shared-key generation apparatus obtains, as the public key, a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate the first encryption information as a polynomial,

the public-key obtaining subunit obtains the public-key polynomial, and the re-encryption subunit generates a decryption verification-value polynomial from the second decryption verification value, generates a decryption blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value

polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the decryption blind-value polynomial to randomize the decryption verification-value polynomial, to generate the re-encryption information as a polynomial.

**44. (Original)** The shared-key recovery apparatus of claim 24, wherein the judging unit compares the first decryption verification value and the second decryption verification value, thereby judging that the decryption shared key should be outputted if the first decryption verification value is identical to the second decryption verification value.

**45. (Currently Amended)** The shared-key recovery apparatus of claim 24, wherein the shared-key generation apparatus further obtains a content, encrypts the content using the shared key to generate an encrypted content, and transmits the encrypted content, the receiving unit further receives the encrypted content, and the shared-key recovery apparatus further comprises:  
a decryption unit ~~operable~~ configured to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content; and  
an outputting unit ~~operable~~ configured to output the decrypted content.

**46. (Currently Amended)** A shared-key generating method used in a shared-key generation apparatus ~~that notifies a shared-key recovery apparatus about a shared key, in secrecy,~~ the shared-key generating method comprising:

~~a seed value generating step of~~ generating a seed value;

~~a shared-key generating step of generating a verification value and a shared key,~~  
from the seed value;

~~a first encryption step of encrypting the verification value to generate first~~  
encryption information;

~~a second encryption step of encrypting the seed value based on the verification~~  
value, to generate second encryption information; and

~~a transmitting step of transmitting~~ to a shared-key recovery apparatus the first  
encryption information and the second encryption information without transmitting to the  
shared-key recovery apparatus the generated shared-key,

wherein the shared-key recovery apparatus decrypts the first encryption  
information to generate a first decryption verification value, decrypts the second  
encryption information based on the first decryption verification value to generate a  
decryption seed value, generates a second decryption verification value and a decryption  
shared key from the decryption seed value according to the same method as used in the  
shared-key generating unit of the shared-key generation apparatus, judges whether the first  
decryption verification value is identical to the second decryption verification value, and  
judges that the generated decryption shared key is identical to the shared key generated in  
the shared-key generation apparatus when it is judged that the first decryption verification  
value is identical to the second decryption verification value,

~~wherein the shared-key generation apparatus and the shared-key recovery~~  
~~apparatus are separate apparatuses~~ the shared-key generation apparatus is distinct from  
the shared-key recovery apparatus, and

~~wherein the first encryption information and the second encryption information~~  
~~are separate pieces of information~~ the first encryption information is distinct from the  
second encryption information.

**47. (Currently Amended)** A shared-key generating program used in a shared-key generation apparatus ~~that notifies a shared key recovery apparatus about a shared key, in secrecy,~~ the shared-key generating program causing the shared-key generation apparatus to perform a method comprising:

~~a seed value generating step of generating a seed value;~~

~~a shared key generating step of generating a verification value and a shared key,~~  
from the seed value;

~~a first encryption step of~~ encrypting the verification value to generate first encryption information;

~~a second encryption step of~~ encrypting the seed value based on the verification value, to generate second encryption information; and

~~a transmitting step of transmitting to a shared-key recovery apparatus the first encryption information and the second encryption information~~ without transmitting to the shared-key recovery apparatus the generated shared-key,

wherein the shared-key recovery apparatus decrypts the first encryption information to generate a first decryption verification value, decrypts the second encryption information based on the first decryption verification value to generate a decryption seed value, generates a second decryption verification value and a decryption shared key from the decryption seed value according to the same method as used in the shared-key generating unit of the shared-key generation apparatus, judges whether the first decryption verification value is identical to the second decryption verification value, and judges that the generated decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value,

~~wherein the shared-key generation apparatus and the shared-key recovery apparatus are separated apparatuses~~ the shared-key generation apparatus is distinct from the shared-key recovery apparatus, and

~~wherein the first encryption information and the second encryption information are separate pieces of information~~ the first encryption information is distinct from the second encryption information.

**48. (Canceled)**

**49. (Currently Amended)** A shared-key recovery method used in a shared-key recovery apparatus that receives information regarding a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting to the shared-key recovery apparatus the first encryption information and the second encryption information without transmitting to the shared-key recovery apparatus the generated shared-key, the shared-key recovery method comprising:

~~a receiving step of receiving from the shared-key generation apparatus~~ the first encryption information and the second encryption information;

~~a first decryption step of~~ decrypting the first encryption information, to generate a first decryption verification value;

~~a second decryption step of~~ decrypting the second encryption information based on the first decryption verification value, to generate a decryption seed value;

~~a shared-key generating step of~~ generating a second decryption verification value

and a decryption shared key, from the decryption seed value ~~and~~ according to [[a]] the same method as used in the shared-key generation apparatus;

~~a judging step of judging~~ whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification value; and

judging that the generated decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value, ~~based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted ; and~~

~~an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key,~~

~~wherein the shared key generation apparatus and the shared key recovery apparatus are separated apparatuses~~ the shared-key generation apparatus is distinct from the shared-key recovery apparatus, and

~~wherein the first encryption information and the second encryption information are separate pieces of information~~ the first encryption information is distinct from the second encryption information.

**50. (Currently Amended)** A shared-key recovery program used in a shared-key recovery apparatus that receives information regarding a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a verification value and a shared key from the seed value, encrypting the

verification value to generate first encryption information, encrypting the seed value based on the verification value to generate second encryption information, and transmitting to the shared-key recovery apparatus the first encryption information and the second encryption information without transmitting to the shared-key recovery apparatus the generated shared-key, the shared-key recovery program causing the shared-key recovery apparatus to perform a method comprising:

~~a receiving step of receiving~~ from the shared-key generation apparatus the first encryption information and the second encryption information;

~~a first decryption step of~~ decrypting the first encryption information, to generate a first decryption verification value;

~~a second decryption step of~~ decrypting the second encryption information based on the first decryption verification value, to generate a decryption seed value;

~~a shared key generating step of~~ generating a second decryption verification value and a decryption shared key, from the decryption seed value ~~and~~ according to [[a]] the same method as used in the shared-key generation apparatus;

~~a judging step of judging~~ whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification value; and

judging that the generated decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted ; and

~~an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key,~~

~~wherein the shared key generation apparatus and the shared key recovery apparatus are separated apparatuses~~ the shared-key generation apparatus is distinct from the shared-key recovery apparatus, and

~~wherein the first encryption information and the second encryption information are separate pieces of information~~ the first encryption information is distinct from the second encryption information.

**51. (Canceled)**

**52. (New)** The key agreement system of claim 1, wherein the shared key is generated according to a key generation algorithm of the NTRU cryptosystem, the Diffie-Hellman key agreement protocol being not used in the NTRU cryptosystem.

**53. (New)** The key agreement system of claim 1, wherein  
the judging unit judges that the decryption shared key is not identical to the shared key generated in the shared-key generation apparatus and that the decryption shared key is not used for a decryption, when it is judged that the first decryption verification value is not identical to the second decryption verification value.